



# Marcos de referencia y experiencias en la realización de auditorías y diagnósticos de TIC

Red Universitaria de Colaboración en Ingeniería de Software y Bases de Datos

Mtra. María Teresa Ventura Miranda  
L.A. Heidi Alejandra Pérez Vera

17 de mayo 2022

CONCEPTOS Y TIPOS DE  
AUDITORÍA

01

AUDITORÍAS DE TIC

02

CONCEPTO DE  
DIAGNÓSTICO

03

CONTENIDO

04

AUDITORÍAS Y  
DIAGNÓSTICOS:  
SIMILITUDES Y  
DIFERENCIAS

05

MARCOS DE  
REFERENCIA

06

EXPERIENCIAS

# 01

## Conceptos y tipos de auditoría

---



# Conceptos de Auditoría



## ISO 9000:2015 Fundamentos y vocabulario

Proceso sistemático, **independiente** y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Inspección y verificación **formales** para comprobar si se sigue un estándar o un conjunto de directrices, si los registros son precisos o si se cumplen los objetivos de eficiencia y eficacia.

ISACA



## IEEE 1028:2008 Revisiones y auditorías de software

Una examinación **independiente** del producto o de los procesos de software realizada por alguien externo para evaluar cumplimiento de especificaciones, estándares, acuerdos contractuales, y otros criterios.

# Tipos de Auditoría



Internas



Externas

POR SU ORIGEN



Contable o  
financiera



Operacional



Administrativa



De TIC

POR TEMA



Previo  
a la operación



Durante  
la operación



Posterior a  
la operación

POR EL PERIODO EN EL  
QUE SE REALIZA



# 02

## Auditorías de TIC

---

# Auditorías de TIC

## Auditoría de sistemas de información

Verifica que los sistemas informáticos:

- satisfagan los requerimientos de la organización para los que fueron creados;
- tengan entradas, procesamiento y salidas de información válidas;
- mantengan la integridad, disponibilidad y en su caso confidencialidad de los datos;
- proporcionen información relevante y confiable;
- cuenten con controles internos que eviten, detecten o corrijan de manera oportuna eventos no deseados;
- estén implementados de acuerdo con prácticas aceptables de desarrollo que contribuyan a su calidad y faciliten su mantenimiento;
- estén protegidos y mantengan la continuidad de la operación;
- cumplen con la reglamentación aplicable;

## Auditoría funcional de software

Proporciona una evaluación independiente de los productos de software, verificando que la funcionalidad y el rendimiento reales de sus elementos de configuración sean consistentes con las especificaciones de requisitos. Este tipo de auditorías se realiza antes de la entrega del software o después de la implementación.

# Auditorías de TIC

## **Auditoría de la gestión de recursos de TIC**

Evalúa la adquisición y contratación de bienes y servicios informáticos para determinar si estas fueron realizadas por razones válidas y conforme a las normas administrativas; así como que los recursos adquiridos sean aprovechados y generen los beneficios esperados de acuerdo con lo planificado.

## **Auditoría a las TIC (enfoque de la Auditoría Superior de la Federación)**

Se revisan las adquisiciones, la administración y el aprovechamiento de sistemas e infraestructuras, la calidad de los datos y la seguridad de la información de las entidades públicas.

# Auditorías de TIC

## Auditoría de seguridad

### Técnicas

Análisis de seguridad de los sistemas y de la infraestructura tecnológica para detectar vulnerabilidades de seguridad que podrían ser explotadas y poner en riesgo la seguridad de los activos de la organización.

### De cumplimiento

Verifican la implementación de políticas y procedimientos conforme a las normativas organizacionales o respecto a algún estándar de seguridad (ISO 27001).

## Auditoría forense

Revisión pormenorizada de procesos, hechos y evidencias, con el propósito de documentar la existencia de un presunto acto irregular, las causas que los han producido y su afectación. Por ejemplo: tras un incidente de seguridad informática o una operación irregular en algún sistema de información.



# Auditorías de TIC



## Auditoría de datos

### De base de datos

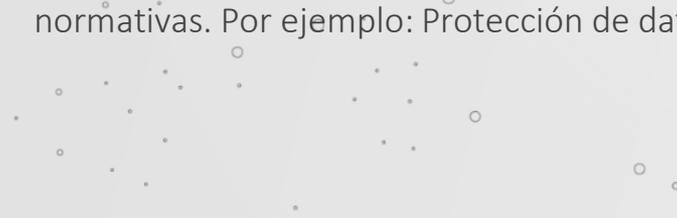
Examina los controles de acceso, almacenamiento, actualización, respaldo, recuperación y destrucción de las bases de datos.

### De calidad de datos

Analiza la integridad, exactitud y completitud de los datos para determinar su calidad así como descubrir y analizar patrones para detectar anomalías.

### De cumplimiento

Verifica la implementación de mecanismos y controles para cumplir con determinadas normativas. Por ejemplo: Protección de datos personales.





# 03

## Concepto de diagnóstico

---

# ¿Qué es un Diagnóstico?

Considera la evaluación de un área, servicio o recurso de TIC contra un conjunto específico de prácticas, marco de trabajo, estándar o metodología.

- Estado actual
- Problemática existente
- Nivel de madurez

# ¿Para qué realizar un diagnóstico?



- Necesidades específicas
- Rutas de acción
- Información que apoye la toma de decisiones

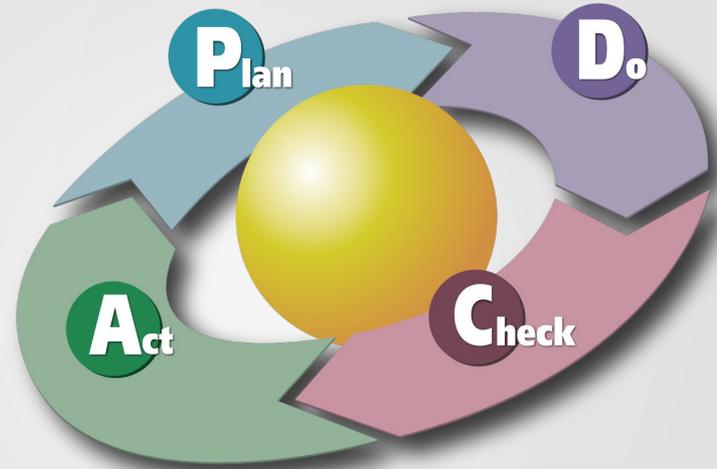


Transmitir el sentido de crecimiento, mejora y valor con relación a métodos de trabajo, calidad y resultados que se buscan con el diagnóstico

# Referentes que consideran los diagnósticos como punto de partida para la mejora

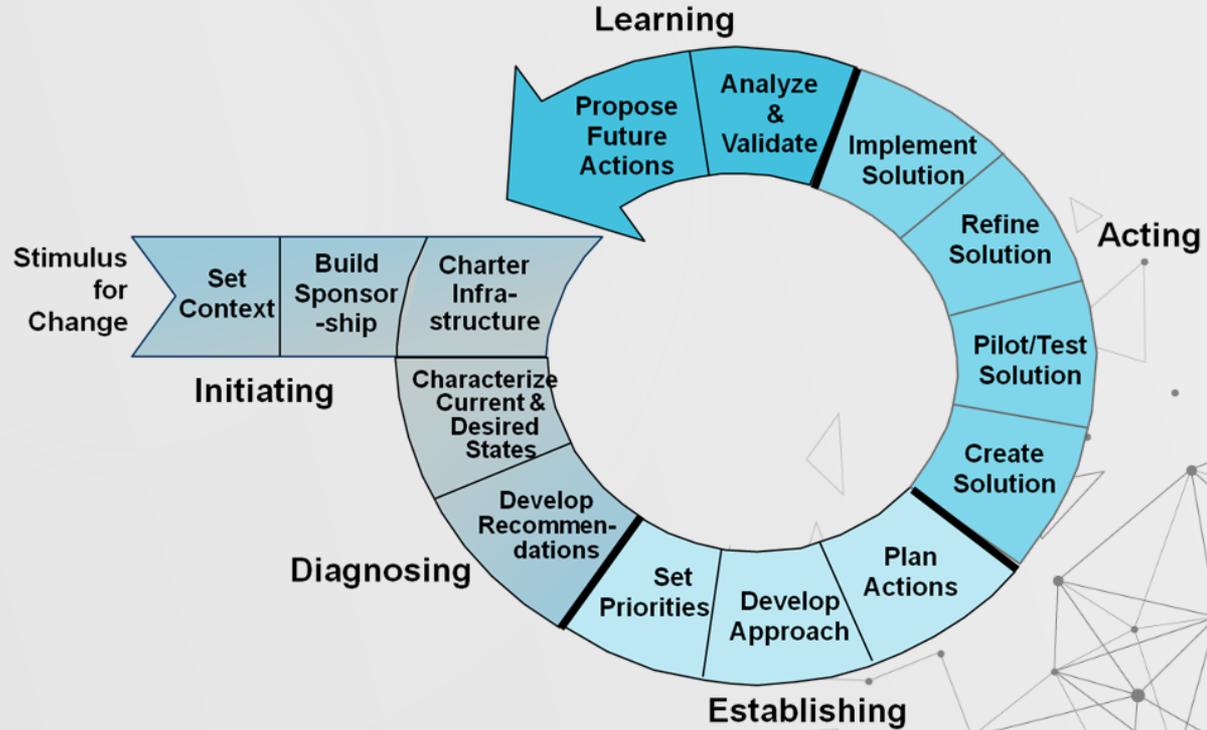
*ISO 9004:2018 Gestión de la calidad — Calidad de una organización — Orientación para lograr el éxito sostenido.*

La autoevaluación puede proporcionar una visión global del desempeño de una organización y del grado de madurez. Puede ayudar a identificar áreas para la mejora y/o innovación y a determinar prioridades para acciones subsiguientes.

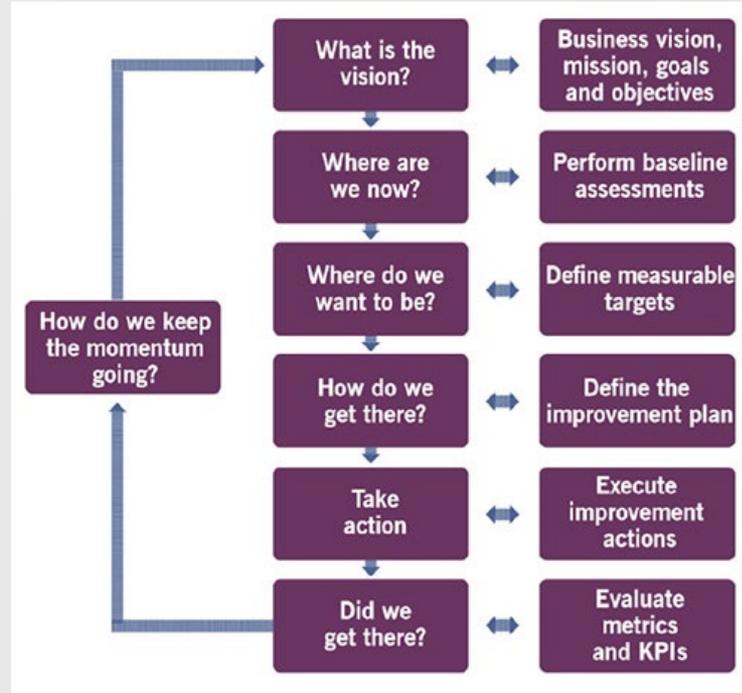


# Modelo IDEAL

IDEAL (Initiating, Diagnosing, Establishing, Acting & Learning, por sus siglas en inglés). Es un modelo de mejora organizacional que sirve como mapa de ruta para implementar acciones de mejora.



# ITIL – Modelo de mejora continua



Principios rectores para la mejora continua

# 04

## Auditorías y diagnósticos: similitudes y diferencias



# Auditorías y diagnósticos: similitudes y diferencias

En general las auditorías y diagnósticos son evaluaciones que permiten identificar cómo se encuentra algún aspecto de una organización en un momento determinado.

Las auditorías tienen un carácter más formal (o incluso legal en algunos casos). Principios:



- Integridad
- Imparcialidad
- Profesional
- Confidencialidad
- Independencia
- Enfoque basado en evidencia
- Enfoque basado en riesgos

# Auditorías y diagnósticos: similitudes y diferencias

Las auditorías se asocian más con una examinación externa, sin embargo también se realizan de manera interna (por ejemplo, en los sistemas de gestión ISO). Los diagnósticos también pueden ser realizados por personal interno a la organización o por personal externo.

Nivel de objetividad



Mismo  
equipo de  
trabajo

Entre  
pares

Otro equipo de  
trabajo de la  
misma  
organización

Externos a la  
organización

# 05

## Marcos de referencia





Inició como un pequeño grupo de personas que auditaba controles en sistemas informáticos en los años 60s y en 1969 se formalizó como la Asociación de Auditores de Procesamiento Electrónico de Datos (Electronic Data Processing Auditors Association, EDPAA). En 1976 formó una fundación educativa para expandir conocimiento en el ámbito de control de TI. Su nombre viene de Information Systems Audit and Control Association.



Certified Information System Auditor.



Certified Information Security Manager.



Certified in the Governance of Enterprise IT



Certified in Risk and Information System Control



Certified Data Privacy Solution Engineering

# Referentes emitidos de ISACA

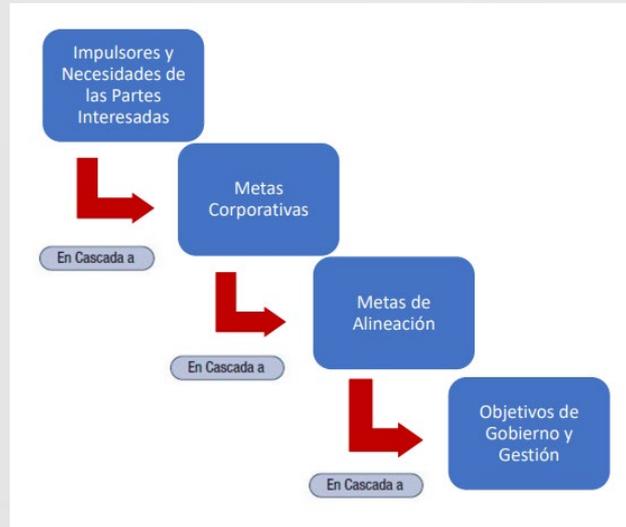
- IT Audit Framework (ITAF)
- COBIT
- CMMI

- Blockchain
- Cloud Computing Management
- DevOps
- eCommerce & Public Key Infrastructure
- IPv6 Security
- IT Business Continuity
- IT Strategic Management
- Manage Programs and Projects
- Manage Suppliers Audit
- Outsourced IT Environments
- Risk IT Framework
- Shadow IT Audit
- Software Assurance Audit
- UNIX/LINUX Operating System Security Audit
- VPN Security Audit
- Otros



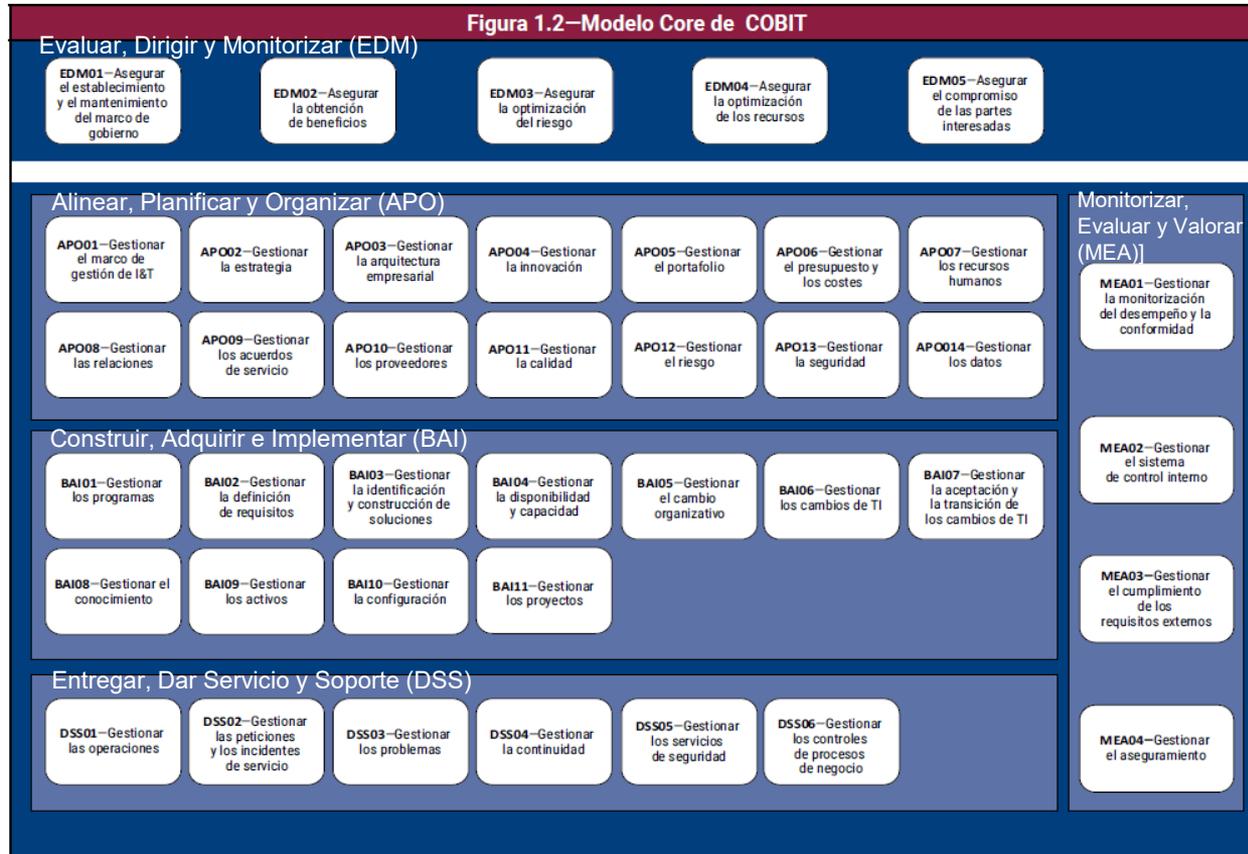
# COBIT

- La primera versión de COBIT surgió en 1996 como un conjunto de objetivos de control para auditar aplicaciones de negocio y ha ido evolucionando. La última versión en el 2019 se define como un marco de trabajo para el gobierno y la gestión de tecnologías de la información que da soporte al logro de las metas organizacionales.



# COBIT

Figura 1.2—Modelo Core de COBIT



Gobierno

Gestión

# COBIT

## (Ejemplo: Gestionar la identificación y construcción de soluciones)

<b>Dominio: Construir, adquirir e implementar</b>	<b>Área prioritaria: Modelo Core de COBIT</b>
<b>Objetivo de gestión: BAI03 – Gestionar la identificación y construcción de soluciones</b>	
<b>Descripción</b>	
Establecer y mantener productos y servicios identificados (tecnología, procesos de negocio y flujos de trabajo) alineados con los requisitos de la empresa que cubran el diseño, desarrollo, adquisición/subcontratación y la asociación con proveedores. Gestionar la configuración, preparación de pruebas, pruebas, gestión de requisitos y mantenimiento de procesos de negocio, aplicaciones, información/datos, infraestructura y servicios.	
<b>Propósito</b>	
Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa.	



<b>Práctica clave de gestión</b>
BAI03.01 Diseño de soluciones de alto nivel.
BAI03.02 Diseñar componentes detallados para la solución.
BAI03.03: Desarrollar los componentes de la solución.
BAI03.04 Adquirir los componentes de la solución.
BAI03.05 Construir soluciones.
BAI03.06 Realizar el aseguramiento de calidad (QA).
BAI03.07 Preparar las pruebas de la solución.
BAI03.08 Ejecutar las pruebas de la solución.
BAI03.09 Gestionar los cambios a los requisitos.
BAI03.10: Mantener las soluciones.
BAI03.11 Definir productos y servicios de TI y mantener el portafolio de servicios.
BAI03.12 Diseñar soluciones conforme a la metodología de desarrollo definida.



<b>Actividades</b>
1. Dentro de un entorno separado, desarrollar el diseño detallado propuesto para los procesos de negocio, servicios de soporte, aplicaciones, infraestructura y repositorios de información.
2. Cuando los terceros están involucrados con el desarrollo de soluciones, garantizar que el mantenimiento, soporte, estándares de desarrollo y el licenciamiento se aborda y se cumple con las obligaciones contractuales.
3. Hacer un seguimiento de las peticiones de cambio y de las revisiones de diseño, desempeño y calidad. Asegurar la participación activa de todas las partes interesadas afectadas.
4. Documentar todos los componentes de la solución conforme a los estándares definidos. Mantener un control de versiones sobre todos los componentes desarrollados y la documentación asociada.
5. Evaluar el impacto de la personalización y configuración de la solución en el rendimiento y la eficiencia de las soluciones adquiridas y en la interoperabilidad con las aplicaciones, sistemas operativos y otra infraestructura existente. Adaptar procesos de negocio cuando sea necesario para aprovechar la capacidad de la aplicación.
6. Garantizar que las responsabilidades de usar componentes de infraestructura de alta seguridad o de acceso restringido estén claramente definidas y sean comprendidas por aquellos que desarrollan e integran los componentes de infraestructura. Es necesario monitorizar e informar sobre su uso.

# COBIT

## (Ejemplo: Gestionar la identificación y construcción de soluciones)

<b>D. Componente: Personas, habilidades y competencias</b>		
<b>Habilidad</b>	<b>Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)</b>	<b>Referencia específica</b>
Desarrollo de aplicaciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.1. Application Development
Pruebas de procesos de negocio	Skills Framework for the Information Age V6, 2015	BPTS
Integración de componentes	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.2. Component Integration
Diseño de la base de datos	Skills Framework for the Information Age V6, 2015	DBDS
Producción de documentación	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.5. Documentation Production
Diseño de hardware	Skills Framework for the Information Age V6, 2015	HWDE
Configuración de portabilidad/ software	Skills Framework for the Information Age V6, 2015	PORT
Programación/desarrollo de software	Skills Framework for the Information Age V6, 2015	PROG
Liberación y despliegue	Skills Framework for the Information Age V6, 2015	RELM
Arquitectura de la solución	Skills Framework for the Information Age V6, 2015	ARCH
Despliegue de soluciones	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.4. Solution Deployment
Diseño de sistemas	Skills Framework for the Information Age V6, 2015	DESN
Gestión del desarrollo de sistemas	Skills Framework for the Information Age V6, 2015	DLMG
Ingeniería de sistemas	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	B. Build—B.6. Systems Engineering

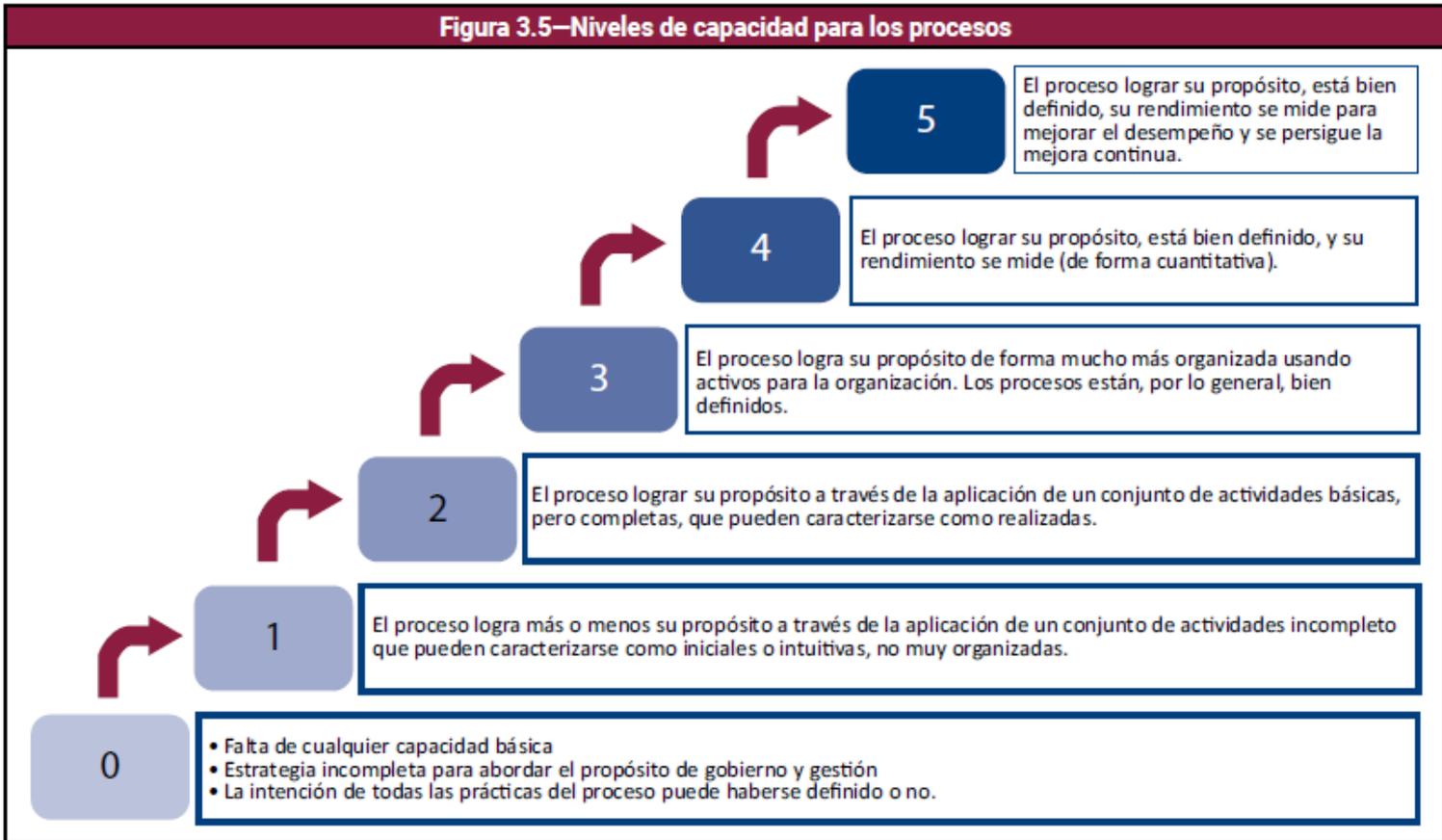
# COBIT

(Ejemplo: Gestionar la identificación y construcción de soluciones)

<b>E. Componente: Políticas y procedimientos</b>			
<b>Política relevante</b>	<b>Descripción de la política</b>	<b>Documentación relacionada</b>	<b>Referencia específica</b>
Política de mantenimiento	Define el soporte adecuado de los componentes de software y hardware para asegurar una mayor vida de los activos, mejorar la productividad de los empleados y mantener una experiencia de usuario aceptable.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.10 Maintenance (MA-1)
Política de desarrollo de software	Estandarizar el desarrollo de software en la organización mediante una lista de todos los protocolos y estándares a seguir.		
Política de adquisición de sistemas y servicios	Proporciona procedimientos para evaluar, revisar y validar los requisitos para la adquisición de sistemas y servicios.	National Institute of Standards and Technology Special Publication 800-53, Revisión 5 (Borrador), agosto de 2017	3.18 System and services acquisition (SA-1)

# COBIT

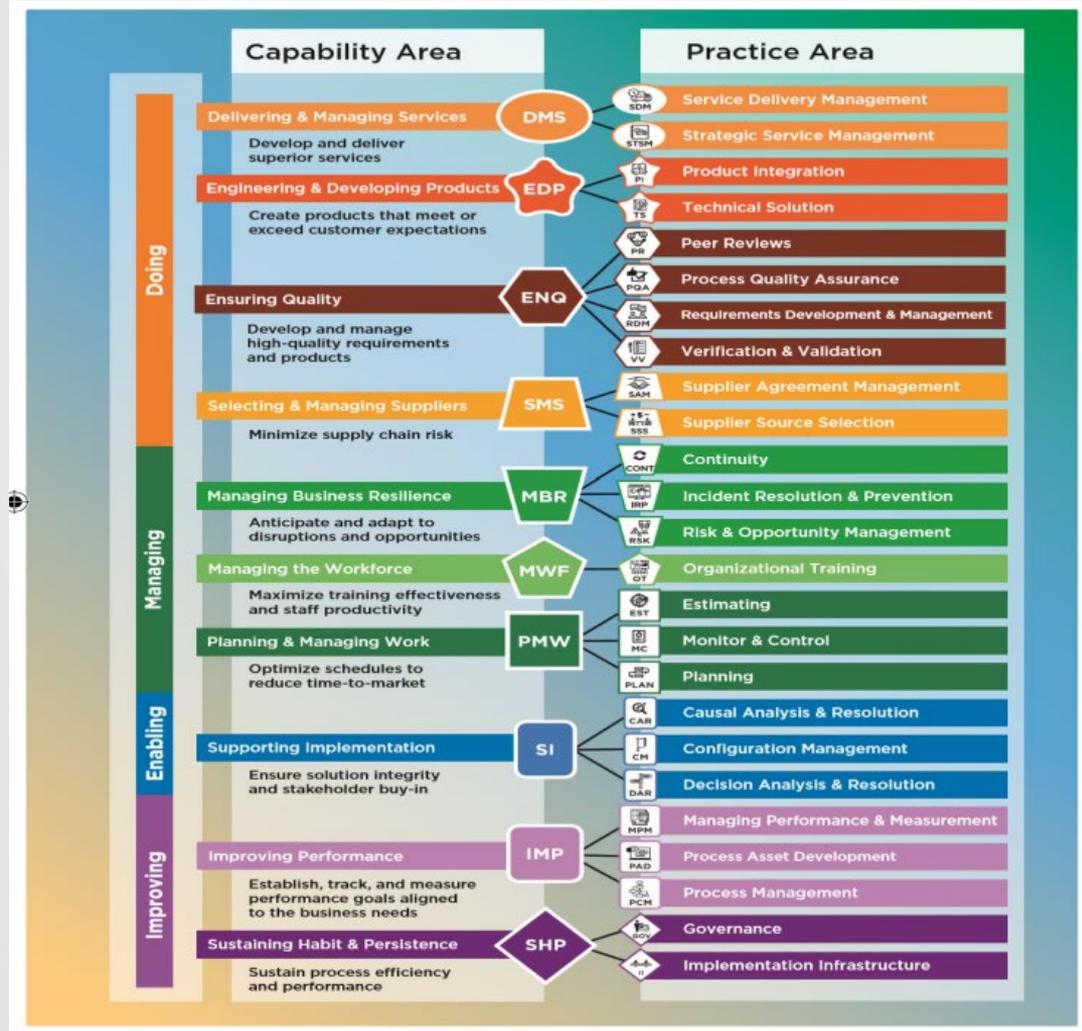
Figura 3.5—Niveles de capacidad para los procesos



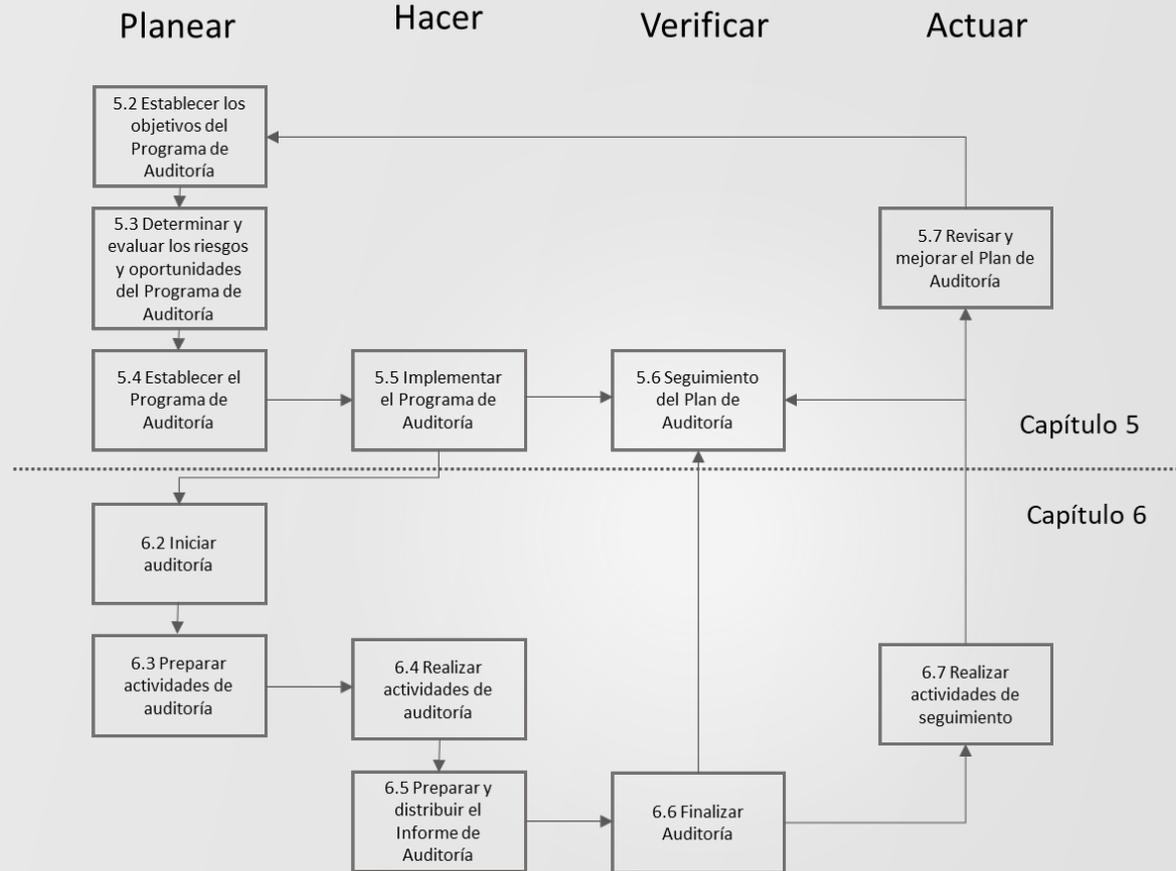
# CMMI

Integración de modelos de madurez de capacidades es un conjunto de prácticas para la mejora de las organizaciones en temas de:

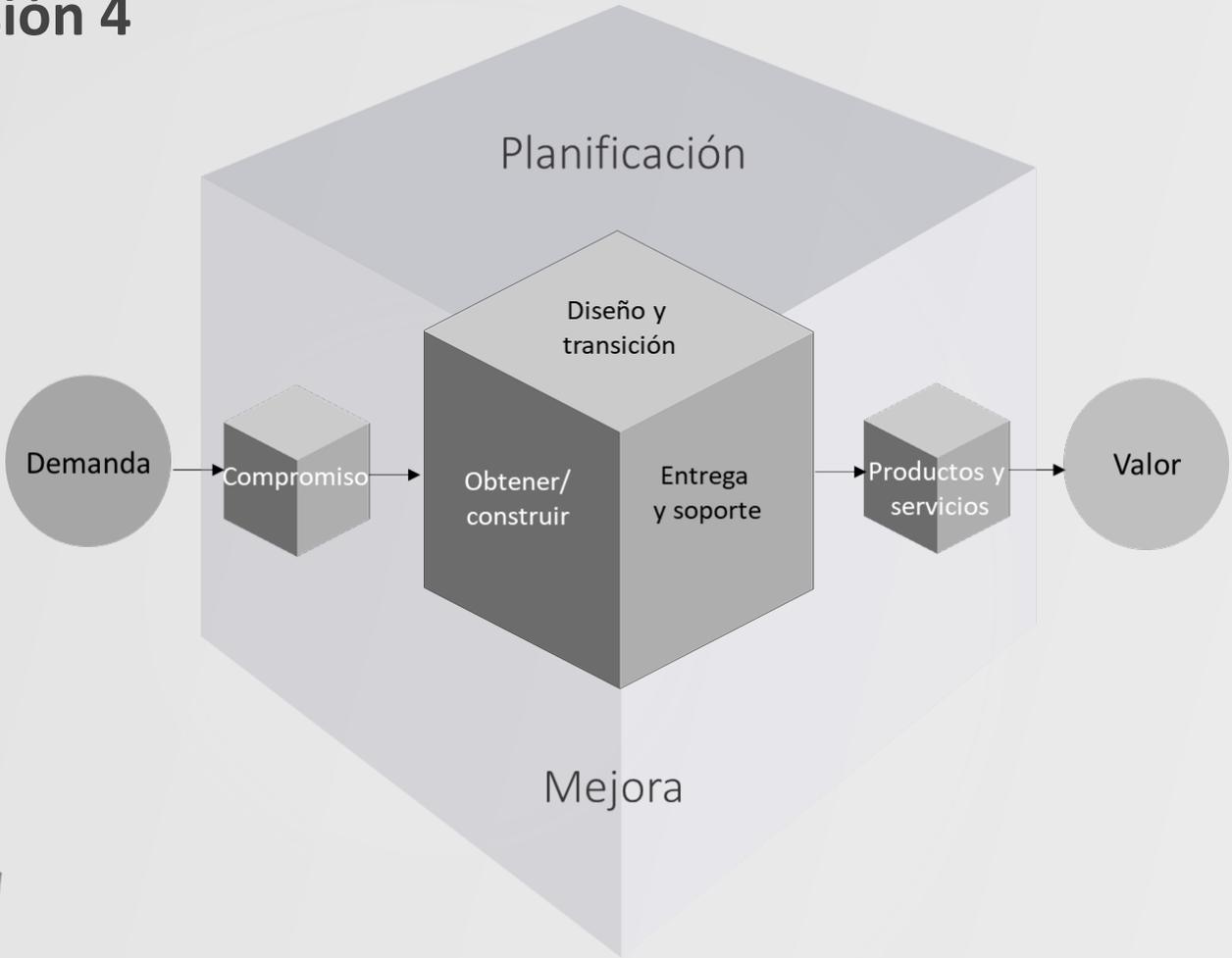
- Desarrollo
- Servicios
- Administración de proveedores



# ISO 19011:2018 – Directrices para la auditoría de los sistemas de gestión



# ITIL – Versión 4



# ITIL – Versión 4

14

PRÁCTICAS DE GESTIÓN  
GENERAL

- Gestión de la arquitectura
- Mejora continua
- Gestión de la seguridad de la información
- Gestión del conocimiento
- Medición y presentación de informes
- Gestión del cambio organizacional
- Gestión de la cartera
- Gestión de proyectos
- Gestión de las relaciones
- Gestión de riesgos
- Gestión financiera de los servicios
- Gestión de la estrategia
- Gestión de proveedores
- Gestión de la fuerza laboral y del talento

17

PRÁCTICAS DE GESTIÓN  
DEL SERVICIO

- Gestión de la disponibilidad
- Análisis del negocio
- Gestión de la capacidad y el rendimiento
- Control de cambios
- Gestión de incidentes
- Gestión de activos de TI
- Monitoreo y gestión de eventos
- Gestión de problemas
- Gestión de versiones
- Gestión de catálogos de servicios
- Gestión de la configuración del servicio
- Gestión de la continuidad del servicio
- Diseño del servicio
- Servicio de atención al cliente
- Gestión del nivel de servicio
- Gestión de solicitudes de servicio
- Validación y prueba del servicio

03

PRÁCTICAS DE  
GESTIÓN TÉCNICA

- Gestión de la implementación
- Gestión de infraestructuras y plataformas
- Desarrollo y gestión de software



# ISO 20000:2018 – Gestión de Servicios



# ISO 27001:2018

## Sistema de Gestión de Seguridad de la Información



# Guía PMBOK – 7° edición (ANSI/PMI 99-001-2021)

01



## Stewardship

Gestión diligente, responsable y sostenible

02



## Team

Entorno colaborativo, cultura de respeto

03



## Stakeholders

Compromiso de las partes involucradas

04



## Value

Centrarse en el valor para el cliente

05



## Systems Thinking

Pensamiento sistemático y holístico

06



## Leadership

Liderazgo motivador, entrenar y aprender

07



## Tailoring

La gestión se adapta al contexto

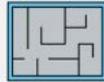
08



## Quality

Incorporar la calidad en procesos y resultados

09



## Complexity

Se aborda con experiencia, conocimiento y aprendizaje

10



## Risk

Abordar oportunidades y amenazas en el ciclo de vida

11



## Adaptability

Resiliencia y adaptación como base de comportamiento

12



## Change

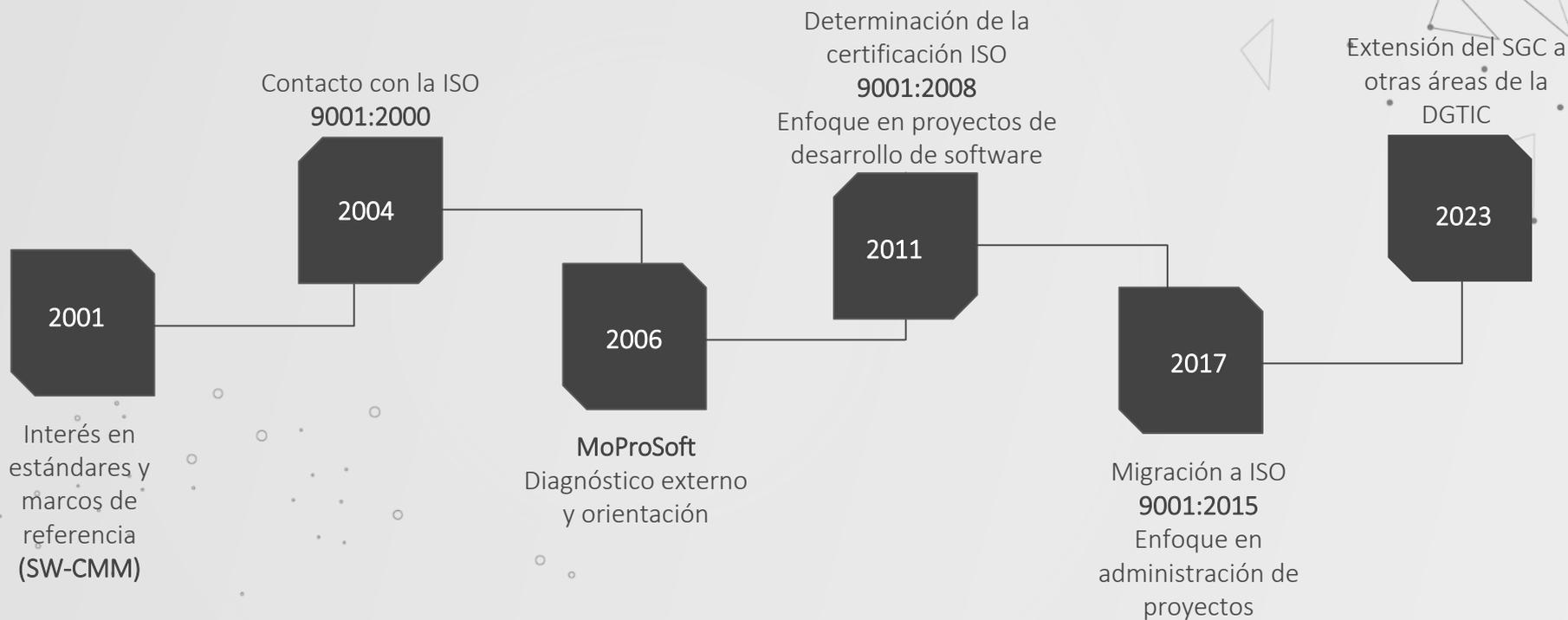
Permitir el cambio para conseguir lo previsto



# 06

## Experiencias

# Sistema de gestión de calidad ISO 9001 de la DCV-DGTIC



# Estudios del estado de las TIC en la UNAM

2017

Diagnóstico de la situación actual y nivel de desarrollo de las TIC en la UNAM

COBIT  
MAAGTICSI  
ISO 38500  
ITIL

2021

3er estudio del nivel de desarrollo de las TIC en entidades y dependencias de la UNAM

Mayor alineación con indicadores de TIC nacionales e internacionales de las Instituciones de Educación Superior

2019

2o estudio del nivel de desarrollo de las TIC en entidades y dependencias de la UNAM.

# Auditoría al Sistema de Voto para Mexicanos Residentes en el Extranjero – INE



DGTIC  
Dirección de Colaboración  
y Vinculación

FES Aragón

DGTIC  
Coordinación de Seguridad  
de la Información

Facultad de Ingeniería

Equipo interdisciplinario de más de 50 personas

La imagen muestra una captura de pantalla de un navegador web que muestra la página de inicio del sistema de voto electrónico por internet del INE. El navegador muestra la URL `votoextranjero.mx/web/vmre/voto-por-internet`. En la parte superior, hay un menú de navegación con el logo del INE y el texto "VOTO RESIDENTES EN EL EXTRANJERO". Debajo del menú, hay un banner con el título "Voto electrónico por internet" y una imagen de una persona votando en un terminal. En la parte inferior, hay un botón que dice "Tema INICIO | VOTO ELECTRÓNICO POR INTERNET" y un texto que dice "Emite tu voto, de manera segura, por la vía electrónica por internet, para la Gubernatura de Aguascalientes, Durango, Oaxaca o Tamaulipas, según sea el caso." y "Si estás registrado para votar por la modalidad electrónica por internet, recibirás tus claves de acceso mediante el correo electrónico que proporcionaste al momento de tu registro. Ejercer tu voto, de acuerdo a las siguientes fechas:".

<https://votoextranjero.mx/web/vmre>

# Auditoría al Sistema de Voto para Mexicanos Residentes en el Extranjero – INE



Lineamientos que establecen las Características Generales que debe cumplir el Sistema de Voto Electrónico por Internet para las y los Mexicanos Residentes en el Extranjero

TÍTULO I DISPOSICIONES GENERALES Capítulo Único De la Naturaleza, Objeto y Ámbito de aplicación

TÍTULO II DEL SISTEMA Capítulo Primero Aspectos Generales del Sistema

Capítulo Segundo Fases para el Desarrollo del Modelo Operativo del Sistema

Sección Primera Creación de la Llave Criptográfica

Sección Segunda De la Apertura del Sistema

Sección Tercera De la Autenticación del Votante

Sección Cuarta Del Monitoreo del Sistema

Sección Quinta Del Cierre del Sistema

Sección Sexta Del Descifrado y Cómputo de los Votos

Sección Séptima Del Resguardo y Preservación de la Información

# Auditoría al Sistema de Voto para Mexicanos Residentes en el Extranjero – INE



Lineamientos para la auditoría al Sistema de Voto Electrónico por Internet para las y los Mexicanos Residentes en el Extranjero del Instituto Nacional Electoral.

## TÍTULO I DISPOSICIONES GENERALES

Capítulo Único De la Naturaleza, Objeto y Ámbito de aplicación

## TÍTULO II DE LOS ASPECTOS METODOLÓGICOS

Capítulo Primero De los Generales de la Auditoría

Capítulo Segundo De la Planeación de la Auditoría

Capítulo Tercero Del Alcance de la Auditoría

Capítulo Cuarto De la Ejecución de la Auditoría Sección Primera De los Generales de la Ejecución

Sección Segunda De las Pruebas al Sistema de Voto Electrónico

Sección Tercera De las Pruebas de Aseguramiento de la Calidad

Sección Cuarta De las Pruebas de Seguridad

Sección Quinta De la Revisión del Manejo de la Información

Sección Sexta Del Cumplimiento de la Normatividad

Capítulo Quinto Del Informe Final y su Contenido

Capítulo Sexto Del Dictamen y su Contenido

Capítulo Séptimo De la Publicación del Dictamen

TÍTULO III DE LOS REQUISITOS DE SELECCIÓN Capítulo Único Aspectos Generales

TÍTULO IV DE LA INTERPRETACIÓN Y LOS CASOS NO PREVISTOS

Capítulo Único Criterios de Interpretación

# Auditorías PREP – Instituto Nacional Electoral



Universidad Nacional Autónoma de México



Auditoría de Software al Sistema del Programa de Resultados Electorales Preliminares 2012



- Convenio Específico de Colaboración
- Boletín UNAM-DGCS-050
- Revisión del código fuente del sistema del PREP 2012
- Pruebas funcionales
- Validación del código auditado

**Resultados**

- Informe de la aplicación de recomendaciones de la revisión de código fuente y de las pruebas funcionales de caja negra del PREP 2012
- Boletín UNAM-DGCS-401: Concluye la UNAM la Auditoría de Software y comprueba funcionamiento del sistema del PREP 2012
- Aportaciones y costos
- Conceptos y definiciones
- Materiales recomendados

Contacto

## CELEBRAN INE Y UNAM CONVENIO PARA AUDITORÍA Y APOYO TÉCNICO AL PREP 2015

• La Universidad analiza el sistema informático del PREP 2015 para evaluar la integridad en el procesamiento de la información y la correcta generación de los resultados preliminares del proceso electoral federal 2015.

En el marco del Proceso Electoral Federal 2015, el Instituto Nacional Electoral (INE) y la Universidad Nacional Autónoma de México (UNAM) celebraron un convenio de colaboración para llevar a cabo la auditoría, revisión y apoyo técnico al sistema informático del Programa de Resultados Electorales Preliminares (PREP) 2015.

El PREP es el mecanismo que recaba y publica los resultados electorales preliminares, no definitivos y de carácter estrictamente informativo, mediante la captura de la información asentada en cada una de las actas de escrutinio y cómputo de las casillas ubicadas en todos los distritos electorales. Uno de los elementos medulares de este programa es el sistema informático que se emplea para la captura, transmisión y publicación de resultados vía Internet.

De acuerdo con el Capítulo V de los Lineamientos del PREP, aprobados por el Consejo General del INE el 19 de noviembre de 2014, los sistemas informáticos del PREP deben someterse a una auditoría, con la finalidad de evaluar la integridad de la información durante su procesamiento y la correcta generación de los resultados conforme a la normatividad vigente.

Según se establece en el convenio, la UNAM es la instancia encargada de realizar la auditoría del PREP para la elección de diputados federales 2015. Por ello, la UNAM analiza el aplicativo del PREP 2015 mediante la revisión del código fuente y pruebas de caja negra, para verificar que tanto los datos como las imágenes de las Actas de Escrutinio y Cómputo se procesen de manera íntegra, es decir, que no sufran alteraciones. En el mismo sentido, se está llevando a cabo una revisión para identificar posibles vulnerabilidades en la infraestructura tecnológica del PREP y emitir recomendaciones que permitan subsanarlas oportunamente.

Además de las actividades de auditoría de software previas al día de la elección, durante la operación del PREP se corroborará que los programas en funcionamiento tengan plena correspondencia con los auditados por la Universidad y que las bases de datos no cuenten con información previa antes de su puesta en operación.

De este modo, una vez más la UNAM contribuirá activamente a la integridad, certeza y confiabilidad de los resultados de los comicios federales que se celebrarán el próximo 7 de junio de 2015.

La UNAM, como institución académica reconocida a nivel internacional, cuenta con amplia experiencia en esta materia al haber realizado las auditorías de los sistemas del PREP en los procesos electorales federales de 2009 y 2012 organizados por el entonces Instituto Federal Electoral (IFE).



## PREP Federal 2018 será auditado por la UNAM

ESCRITO POR:  
INE

Número: 003

- Se realizarán verificaciones técnicas a su funcionamiento



La Universidad Nacional Autónoma de México (UNAM) llevará a cabo una auditoría de tecnologías de información y comunicación para el Programa de Resultados Electorales Preliminares (PREP) que utilizará el Instituto Nacional Electoral (INE) en los comicios federales de 2018.

Ambas instituciones firmaron un convenio de colaboración para que la UNAM realice diversas pruebas sobre el sistema informático y la infraestructura tecnológica del PREP, en donde se podrá consultar el avance de los resultados preliminares, no definitivos, de los comicios en los que se elegirá la Presidencia de la República, 128 senadurías y 500 diputaciones federales.

La auditoría estará a cargo de especialistas en software y en seguridad de la información designados por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM, dependencia responsable del proyecto.

En la revisión se realizarán pruebas funcionales de caja negra para validar que el sistema informático del PREP Federal presente la información e imágenes de las actas de escrutinio y cómputo que se capturan en él.

El día de la elección –el 1° de julio–, antes de que empiece a operar el PREP Federal, la UNAM verificará que el sistema corresponde al auditado y que su base de datos no contenga resultados preliminares.

Se revisará la seguridad informática de infraestructura tecnológica del INE así como la del PREP Federal, y se probará la disponibilidad del portal del Instituto y del PREP de las elecciones federales en situaciones de alta demanda.

Además del mismo día se llevará a cabo un monitoreo de seguridad de la red del PREP de los comicios federales para identificar posibles ataques informáticos.

# Referencias

- Auditoría Superior de la Federación. (2022). Tipos y Enfoques de Auditoría. [https://www.asf.gob.mx/Section/53\\_Tipos\\_de\\_auditorias\\_desarrolladas](https://www.asf.gob.mx/Section/53_Tipos_de_auditorias_desarrolladas)
- IEEE Computer Society. (2008). IEEE Standard for Software Reviews and Audits. <https://standards.ieee.org/ieee/1028/4402/>
- ISACA. (2022). Frameworks, Standards and Models. <https://www.isaca.org/resources/frameworks-standards-and-models>
- ISACA. (2020). IT Audit Framework (ITAF).
- ISACA. (2018). Marco de referencia COBIT 2019. Objetivos de gobierno y gestión.
- Person. (2019). Itil guiding principles for continual improvement. Axelos. <https://www.axelos.com/resource-hub/white-paper/itil-guiding-principles-for-continual-improvement>
- Software Engineering Institute. (2009). The IDEAL Model. [https://resources.sei.cmu.edu/asset\\_files/Presentation/2001\\_017\\_001\\_23277.pdf](https://resources.sei.cmu.edu/asset_files/Presentation/2001_017_001_23277.pdf)
- UNAM-DGTIC. (2021). Red de Responsables TIC (REDTIC) - Experiencias TIC en la UNAM <https://www.red-tic.unam.mx/experienciastic>
- UNAM-DGTIC. (2018). Guía para la elaboración de Diagnósticos Informáticos [https://www.red-tic.unam.mx/recursos/2018/2018\\_Guia\\_DireccionGeneralComputoTecnologiasInformacionComunicacion\\_01.pdf](https://www.red-tic.unam.mx/recursos/2018/2018_Guia_DireccionGeneralComputoTecnologiasInformacionComunicacion_01.pdf)



---

# Gracias

Mtra. María Teresa Ventura Miranda  
[tventura@unam.mx](mailto:tventura@unam.mx)

L.A. Heidi Alejandra Pérez Vera  
[heidipv@unam.mx](mailto:heidipv@unam.mx)



---



# Gracias

Mtra. María Teresa Ventura Miranda  
[tventura@unam.mx](mailto:tventura@unam.mx)

L.A. Heidi Alejandra Pérez Vera  
[heidipv@unam.mx](mailto:heidipv@unam.mx)

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.